

#2

PATENT
81800.0165
Express Mail Label No. EL 894 944 710 US

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Yoshifumi TANIMOTO

Serial No: Not assigned

Filed: August 15, 2001

For: FACSIMILE APPARATUS AND FACSIMILE
COMMUNICATION METHOD

Art Unit: Not assigned

Examiner: Not assigned

jc971 U.S. PTO
09/931675
08/15/01

TRANSMITTAL OF PRIORITY DOCUMENT

Box PATENT APPLICATION
Assistant Commissioner for Patents
Washington, D.C. 20231

Dear Sir:

Enclosed herewith is a certified copy of Japanese patent application No. 2000-256261 which was filed August 25, 2000, from which priority is claimed under 35 U.S.C. § 119 and Rule 55.

Acknowledgment of the priority document(s) is respectfully requested to ensure that the subject information appears on the printed patent.

Respectfully submitted,

HOGAN & HARTSON L.L.P.

Date: August 15, 2001

By: Michael Crapenhof
Michael Crapenhof
Registration No. 37,115
Attorney for Applicant(s)

500 South Grand Avenue, Suite 1900
Los Angeles, California 90071
Telephone: 213-337-6700
Facsimile: 213-337-6701

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

Jc971 U.S. PTC
09/931675
08/15/01

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office.

出 願 年 月 日
Date of Application:

2000年 8月25日

願 番 号
Application Number:

特願2000-256261

願 人
Applicant(s):

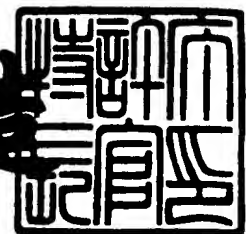
村田機械株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2001年 3月 2日

特許庁長官
Commissioner,
Patent Office

及 川 耕 造



出証番号 出証特2001-3012721

【書類名】 特許願

【整理番号】 21414

【提出日】 平成12年 8月25日

【あて先】 特許庁長官殿

【国際特許分類】 H04N 1/00
H04L 9/14

【発明の名称】 ファクシミリ装置

【請求項の数】 3

【発明者】

【住所又は居所】 京都府京都市伏見区竹田向代町 1 3 6 番地 村田機械株式会社 本社工場内

【氏名】 谷本 好史

【特許出願人】

【識別番号】 000006297

【氏名又は名称】 村田機械株式会社

【代表者】 村田 純一

【代理人】

【識別番号】 100078868

【弁理士】

【氏名又は名称】 河野 登夫

【電話番号】 06-6944-4141

【選任した復代理人】

【識別番号】 100114557

【弁理士】

【氏名又は名称】 河野 英仁

【電話番号】 06-6944-4141

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9805283

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 ファクシミリ装置

【特許請求の範囲】

【請求項 1】 自身及び通信相手の各固有情報に基づく暗号鍵により暗号化／復号しネットワークを介してコンピュータと通信し、該コンピュータの指示でファクシミリ通信を行なうファクシミリ装置であって、親展受信したときに親展処理すべきコンピュータへ通知する手段と、該コンピュータからの要求に応じて親展受信の内容を送信する手段とを備えることを特徴とするファクシミリ装置。

【請求項 2】 自身及び通信相手の各固有情報に基づく暗号鍵により暗号化／復号しネットワークを介してコンピュータと通信し、該コンピュータの指示でファクシミリ通信を行なうファクシミリ装置であって、親展受信したときに親展処理すべきコンピュータへ親展受信の内容を電子メールとして送信する手段を備えることを特徴とするファクシミリ装置。

【請求項 3】 前記親展処理すべきコンピュータと通信する内容の内、前記暗号鍵により暗号化する部分を選択する手段を更に備え、該手段の選択に従って暗号化すべくなしてある請求項 1 又は 2 記載のファクシミリ装置。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、電話回線網を介して通常のファクシミリ通信を行なう機能を有することは勿論のこと、コンピュータネットワーク経由で他のコンピュータに接続されるファクシミリ装置に関するものである。

【 0 0 0 2 】

【従来の技術】

近年、LAN (Local Area Network) 等のコンピュータネットワークに接続することが可能であって、同様にコンピュータネットワークに接続されている他のコンピュータのファクシミリサーバとして機能するファクシミリ装置が開発されている。これは、一般の電話回線網を介しての通常のファクシミリ送受信機能に加えて、コンピュータネットワークに接続された他のコンピュータからの指示で

原稿をファクシミリ送信し、またファクシミリ受信した情報をコンピュータネットワーク経由で他のコンピュータへ配信することが可能なファクシミリ装置である。

【 0 0 0 3 】

従来、ファクシミリ装置はそれを利用するユーザの日常の活動領域内、例えばユーザが仕事をしているオフィス内等に設置されることが多かった。その理由は、原稿を送信する際には直接ファクシミリ装置に原稿をセットする必要がある、また着信があった際には可及的速やかにそれを認識する必要があったからである。しかし、前述のようなコンピュータネットワークに接続されたファクシミリ装置では、ユーザの手許にあるコンピュータで送信の指示を与えることが可能であり、また着信した場合にもユーザの手許のコンピュータへ送信されるため、ユーザの日常の活動領域内に設置される必要は必ずしもない。

【 0 0 0 4 】

ところで、従来のファクシミリ装置では、受信した情報を一旦記憶しておき、親展受信を知らせるリストを印字し、予め定めてあるパスコードが入力されたときに、記憶しておいた情報を印字する親展受信機能を備えている。上述したファクシミリサーバとして機能するファクシミリ装置においても、受信し一旦記憶した情報の宛先コンピュータへメールにより通知し、そのメールを見たユーザがコンピュータから、その記憶しておいた情報を印字させるように、また、自分のメールボックスへ送信させるように、それぞれ指示することが出来る親展受信機能を備えたものが考えられている。ユーザは、また、自動的にメールで送信するように、親展受信がある都度送信するように、何通か溜まったときに送信するように、指定時刻になったときに送信するように、それぞれ設定しておくことが可能である。

【 0 0 0 5 】

【発明が解決しようとする課題】

一般の電話回線網を介しての通常のファクシミリ通信では、通信の秘密が維持されているが、LAN等のコンピュータネットワークでは、通信の秘密は保証されておらず、親展受信した情報でも、コンピュータネットワークを通じて宛先コ

ンピュータへ送信している間に、第三者に盗まれる虞があり、また、宛先コンピュータと送受信する通信文に含まれる秘密にしておきたい情報が盗まれる虞もある。

【 0 0 0 6 】

本発明は、以上のような事情に鑑みてなされたものであり、ファクシミリ通信により親展受信した情報をその宛先コンピュータへ送信する際に、秘密を維持することが出来るファクシミリ装置を提供することを目的とする。

【 0 0 0 7 】

【課題を解決するための手段】

第 1 発明に係るファクシミリ装置は、自身及び通信相手の各固有情報に基づく暗号鍵により暗号化／復号しネットワークを介してコンピュータと通信し、該コンピュータの指示でファクシミリ通信を行なうファクシミリ装置であって、親展受信したときに親展処理すべきコンピュータへ通知する手段と、該コンピュータからの要求に応じて親展受信の内容を送信する手段とを備えることを特徴とする。

【 0 0 0 8 】

このファクシミリ装置では、自身及び通信相手の各固有情報に基づく暗号鍵により暗号化／復号しネットワークを介してコンピュータと通信し、コンピュータの指示でファクシミリ通信を行なう。通知する手段が、親展受信したときに親展処理すべきコンピュータへ暗号化して通知し、送信する手段は、親展処理すべきコンピュータからの暗号化による要求に応じて、親展受信の内容を暗号化して送信する。

これにより、ファクシミリ通信により親展受信した情報をその宛先コンピュータへ送信する際に、秘密を維持することが出来るファクシミリ通信を実現することが出来る。

【 0 0 0 9 】

第 2 発明に係るファクシミリ装置は、自身及び通信相手の各固有情報に基づく暗号鍵により暗号化／復号しネットワークを介してコンピュータと通信し、該コンピュータの指示でファクシミリ通信を行なうファクシミリ装置であって、親展

受信したときに親展処理すべきコンピュータへ親展受信の内容を電子メールとして送信する手段を備えることを特徴とする。

【0010】

このファクシミリ装置では、自身及び通信相手の各固有情報に基づく暗号鍵により暗号化／復号しネットワークを介してコンピュータと通信し、コンピュータの指示でファクシミリ通信を行なう。送信する手段は、親展受信したときに親展処理すべきコンピュータへ親展受信の内容を暗号化して電子メールとして送信する。

これにより、ファクシミリ通信により親展受信した情報をその宛先コンピュータへ送信する際に、秘密を維持することが出来るファクシミリ通信を実現することが出来る。

【0011】

第3発明に係るファクシミリ装置は、前記親展処理すべきコンピュータと通信する内容の内、前記暗号鍵により暗号化する部分を選択する手段を更に備え、該手段の選択に従って暗号化すべくなくしてあることを特徴とする。

【0012】

このファクシミリ装置では、選択する手段が、親展処理すべきコンピュータと通信する内容の内、暗号鍵により暗号化する部分を選択し、その選択に従って暗号化するように構成してあるので、コンピュータネットワークの秘密保証の程度及び親展受信するであろう情報の内容に応じて、秘密保持の程度を定めることが出来る。

【0013】

【発明の実施の形態】

以下に、本発明をその実施の形態を示す図面に基づいて説明する。

実施の形態1.

図1は、本発明に係るファクシミリ装置の実施の形態1のコンピュータネットワークへの接続形態を示す模式図である。本発明に係るファクシミリ装置であるファクシミリサーバ1は、コンピュータネットワークであるLAN5 (Local Area Network) に接続されている。LAN5には、他のコンピュータであるクライ

アントコンピュータ 4 が接続されている。

LAN 5 においては、バイナリファイル転送 (B F T) する為の Salutation プロトコルにより、ファクシミリサーバ 1 の画データはバイナリデータに変換されて送受信される。

【 0 0 1 4 】

ファクシミリサーバ 1 は、アナログの公衆電話回線網 (P S T N) 3 にも接続されており、LAN 5 により接続されたコンピュータネットワークにおけるクライアントコンピュータ 4 のサーバコンピュータとして機能する。具体的にはファクシミリサーバ 1 は、クライアントコンピュータ 4 からの要求に応じてファクシミリメッセージ (画データ) を P S T N 3 へ送信する機能、及び P S T N 3 から受信したファクシミリメッセージをクライアントコンピュータ 4 へ配信する機能等を少なくとも備えている。

ファクシミリサーバ 1 は、P S T N 3 においては、勧告 T. 3 0 (一般交換電話網における文書ファクシミリ伝送のための手順) に従って作動する。

【 0 0 1 5 】

なお、本発明における電話回線網としては、一般の公衆電話回線網に限定するものではなく、例えば専用電話回線網であってもよい。

また、P S T N 3 にはそれぞれ電話番号が付与された多数のファクシミリ装置 (図 1 では参照符号 2 にて一台のみ示されている) が接続されていることは言うまでもない。

なお、図 1 には 1 台のクライアントコンピュータ 4 が示されているが、最低限 1 台が LAN 5 に接続されていればよい。但し、実際にはより多数のクライアントコンピュータが LAN 5 に接続されている場合が多い。

【 0 0 1 6 】

図 2 は、本発明に係るファクシミリ装置であるファクシミリサーバ 1 の実施の形態 1 の構成を示すブロック図である。このファクシミリサーバ 1 は、CPU 1 0 と、この CPU 1 0 にバスを介して接続された PROM 1 1, RAM 1 2, モデム 1 3 a, NCU 1 3 b, 操作パネル 1 4, ディスプレイ 1 5, スキャナ 1 6, プリンタ 1 7, LAN I / F 1 8 等で構成されている。

【 0 0 1 7 】

PROM 1 1 は、CPU 1 0 が実行する種々のコンピュータプログラムを記憶しており、CPU 1 0 はこのPROM 1 1 に記憶されているコンピュータプログラムに基づいてファクシミリサーバ 1 の動作に必要な種々の処理を実行する。

【 0 0 1 8 】

RAM 1 2 は、DRAM, SRAM, フラッシュメモリ等で構成されており、CPU 1 0 によるコンピュータプログラムの実行時に発生する一時的なデータを記憶するほか、画像メモリとしても機能する。

RAM 1 2 は、また、ファクシミリサーバ 1 及び通信相手の各固有情報に基づき作成された暗号鍵により暗号化／復号する、例えば後述するID-NIKS (ID-based Non-Interactive Key Sharing Scheme) による通信に必要な、ファクシミリサーバ 1 のアドレス（固有情報）、センタから配付され入力された秘密情報及びセンタ公開情報を記憶する。

【 0 0 1 9 】

モデム 1 3 a は、ファクシミリ通信が可能なファックスモデムで構成されている。また、モデム 1 3 a は、バスに接続されたNCU (Network Control Unit) 1 3 b と直接的に接続されている。NCU 1 3 b は、PSTN 3 との回線の閉結及び開放の動作を行なうハードウェアであり、必要に応じてモデム 1 3 a をPSTN 3 と接続する。なお、ISDNインタフェースを備えることにより、デジタルの公衆電話回線網 (ISDN) に接続するように構成してもよいことは言うまでもない。

【 0 0 2 0 】

操作パネル 1 4 は、ユーザがファクシミリサーバ 1 を直接操作するために必要な文字キー、テンキー、短縮ダイヤルキー、ワンタッチダイヤルキー、及び会話予約キー等の機能キーを含む各種キーを備えている。

ディスプレイ 1 5 は、液晶表示装置 (LCD) で構成されており、操作パネル 1 4 からの入力結果及びCPU 1 0 の動作状態等を表示する。尚、ディスプレイ 1 5 としては、CRTディスプレイ等であってもよく、また、タッチパネル方式の表示装置で構成することにより、上述した操作パネル 1 4 の一部又は全部と共

用にすることも可能である。

【0021】

スキャナ16は、カラーCCD等を利用して原稿の内容を画像として読み取り、白黒2値又はカラーに変換したドットイメージデータ（画データ）を出力する。このスキャナ16から出力された画データは一旦RAM12に記憶された後、ファクシミリデータに変換されてモデム13aを介してPSTN3へ、またはLANI/F18を介してLAN5へ出力される。

【0022】

プリンタ17は、電子写真方式等のプリンタ装置で構成されており、スキャナ16からの読み取り内容、ファクシミリ受信したイメージデータ（画データ）、及びCPU10が出力する各種のメッセージ等を印字出力する。

LANI/F18は、ファクシミリサーバ1をLAN5と接続するためのインタフェースである。

【0023】

本発明に係るファクシミリ装置の実施の形態1としてのファクシミリサーバ1は基本的には以上の如きハードウェア構成を有しており、通常のファクシミリサーバとしての機能を有しているが、その他に親展受信したときに、例えばID-NIKSによる暗号化／復号によりクライアントコンピュータ4と通信する。

【0024】

ID-NIKSは、各エンティティ（実体；人、コンピュータ、ファクシミリサーバ等）の住所、氏名、名称等の個体を特定するID（Identity）情報を利用する暗号系である。この暗号系では、ID情報に基づいて送受信者間で共通の暗号化鍵を生成するが、予備通信が不要であるので、利便性が高い。

ID-NIKSは、通信相手のID情報を用いて予備通信を行うことなく暗号化鍵を共有する方式であり、送受信者間で公開鍵、秘密鍵を交換する必要がなく、また鍵のリスト及び第三者によるサービスも必要としない方式であり、任意のエンティティ間で安全に通信を行うことが出来る。

【0025】

図3は、このID-NIKSのシステムの原理を説明する為の説明図である。

信頼できるセンタの存在を仮定し、このセンタを中心にして共通鍵生成システムを構成している。エンティティ X の名前、住所、電話番号等の ID 情報は、ハッシュ関数 $h(\cdot)$ を用いて $h(ID_X)$ で表す。センタは任意のエンティティ X に対して、センタ公開情報 $\{PC_i\}$ 、センタ秘密情報 $\{SC_i\}$ 及びエンティティ X の ID 情報 $h(ID_X)$ に基づいて、以下のように秘密情報 S_{Xi} を計算し、秘密裏にエンティティ X へ配布する。

$$S_{Xi} = F_i(\{SC_i\}, \{PC_i\}, h(ID_X))$$

【0026】

エンティティ X は他の任意のエンティティ Y との間で、暗号化、復号のための共有鍵 K_{XY} を、エンティティ X 自身の秘密情報 $\{S_{Xi}\}$ 、センタ公開情報 $\{PC_i\}$ 及び相手先のエンティティ Y の ID 情報 $h(ID_Y)$ を用いて以下のように生成する。

$$K_{XY} = f(\{S_{Xi}\}, \{PC_i\}, h(ID_Y))$$

また、エンティティ Y も同様にエンティティ X への鍵を共通鍵 K_{YX} として生成する。もし常に $K_{XY} = K_{YX}$ の関係が成立すれば、この鍵 K_{XY} 、 K_{YX} をエンティティ X、Y 間で暗号化鍵、復号鍵として使用できる。

【0027】

公開鍵暗号系では、例えば RSA 暗号系の場合にその公開鍵の長さは現在の電話番号の十数倍となり、極めて煩雑である。これに対して、ID-NIKS では、各 ID 情報を名簿という形式で登録しておけば、この名簿を参照して任意のエンティティとの間で共通鍵を生成することができる。

【0028】

ファクシミリサーバ 1 及びクライアントコンピュータ 4 は、予め、センタにおいて、センタ公開情報 $\{PC_i\}$ 、センタ秘密情報 $\{SC_i\}$ 及びそれぞれの LAN 5 におけるアドレスである ID 情報 $h(ID_X)$ に基づいて、それぞれ秘密情報 S_{Xi} が計算され、秘密裏に配布され、記憶している。

ファクシミリサーバ 1 及びクライアントコンピュータ 4 は、LAN 5 における通信において、その通信相手との間で、暗号化、復号のための共通鍵 K_{XY} を、自身の秘密情報 $\{S_{Xi}\}$ 、センタ公開情報 $\{PC_i\}$ 及び相手先の ID 情報 $h(I$

D_Y) を用いて以下のように生成する。

$$K_{XY} = f(\{S_{Xi}\}, \{PC_i\}, h(ID_Y))$$

【0029】

以下に、このような構成のファクシミリサーバ1の動作を、それを示すフローチャートを参照しながら説明する。

図4は、ファクシミリサーバ1が親展受信したときの動作を示すフローチャートであり、図5は、そのときのクライアントコンピュータ4の動作を示すフローチャートである。

ファクシミリサーバ1は、ファクシミリ装置2からPSTN経由で親展受信すると(図4S2)、自身の秘密情報、センタ公開情報、及びその親展受信の宛先である親展処理すべきクライアントコンピュータ4のLAN5におけるアドレスを用いて、暗号化、復号のための共通鍵を作成する(S4)。

【0030】

次に、ファクシミリサーバ1は、クライアントコンピュータ4へ親展受信したことを通知する為の通知文を、作成した共通鍵(S4)により暗号化し(S5)、暗号化した通知文をLAN5経由でクライアントコンピュータ4へ送信する(S6)。

【0031】

クライアントコンピュータ4は、LAN5経由でファクシミリサーバ1から受信すると(図5S20)、自身の秘密情報、センタ公開情報、及びその受信した情報の送信元であるファクシミリサーバ1のLAN5におけるアドレスを用いて、暗号化、復号のための共通鍵を作成する(S22)。

次に、クライアントコンピュータ4は、受信した情報(S20)を、作成した共通鍵(S22)により復号して表示する(S24)。

【0032】

クライアントコンピュータ4は、受信した情報(S20)を復号して表示している(S24)状態で、ユーザによりその応答内容が入力されると(S26)、その応答内容を、作成した共通鍵(S22)により暗号化し(S28)、暗号化した応答内容をLAN5経由でファクシミリサーバ1へ送信する(S30)。

クライアントコンピュータ4は、受信した情報（S20）を復号して表示している（S24）状態で、ユーザによりその応答内容が入力されないままに（S26）、所定時間が経過したときは（S38）リターンする。

【0033】

ファクシミリサーバ1は、LAN5経由でクライアントコンピュータ4から応答内容を受信すると（図4 S8）、作成した共通鍵（S4）により、その応答内容を復号する（S10）。

ファクシミリサーバ1は、復号した応答内容（S10）が、親展受信した画データ（S2）の配信要求であれば（S12）、テキストデータ部分のみを暗号化するように設定されている場合は（S14）、親展受信した画データ（S2）に付属する送信元名称及び送信時刻等のテキストデータのみを暗号化し（S19）、画データと共にクライアントコンピュータ4へ送信し（S17）リターンする。

ファクシミリサーバ1は、LAN5経由でクライアントコンピュータ4から応答内容を受信しない状態で（S8）、所定時間が経過したときは（S18）リターンする。

【0034】

ファクシミリサーバ1は、暗号化する部分が特に設定されていない場合は（S14）、親展受信した画データ（S2）及びそれに付属する送信元名称及び送信時刻等のテキストデータを、作成した共通鍵（S4）により暗号化して（S16）クライアントコンピュータ4へ送信し（S17）リターンする。

ファクシミリサーバ1は、復号した応答内容（S10）が、親展受信した画データ（S2）の配信要求でなければ（S12）リターンする。

【0035】

クライアントコンピュータ4は、LAN5経由でファクシミリサーバ1へ送信した応答内容（図5 S30）が、親展受信した画データ（図4 S2）の配信要求でなければ（図5 S32）リターンし、配信要求であれば（S32）、ファクシミリサーバ1から受信するように待機する（S33）。

【0036】

クライアントコンピュータ 4 は、ファクシミリサーバ 1 から受信したとき（S 3 3）、受信データが暗号化されているときは（S 3 4）、作成した共通鍵（S 2 2）により、その受信データを復号し画像に変換して表示し（S 3 5）リターンする。受信データが暗号化されていないときは（S 3 4）、その受信データをそのまま画像に変換して表示し（S 3 6）リターンする。

尚、クライアントコンピュータ 4 から配信要求するとき、パスコードも入力して送信し、ファクシミリサーバ 1 側でそのパスコードの正誤を判定し、正しいと判定したときに、画データを送信するようにしても良い。

【 0 0 3 7 】

実施の形態 2.

図 6 は、本発明に係るファクシミリ装置の実施の形態 2 のコンピュータネットワークへの接続形態を示す模式図である。本発明に係るファクシミリ装置であるファクシミリサーバ 1 は、コンピュータネットワークである LAN 5（Local Area Network）に接続されている。LAN 5 には、他のコンピュータであるクライアントコンピュータ 4、及び LAN 5 内で送受信される電子メールを仲介する為のメールサーバ 6 が接続されている。

LAN 5 においては、電子メールを送受信する為の SMTP（Simple Mail Transfer Protocol）及び POP 3（Post Office Protocol ver.3）により、ファクシミリサーバ 1 の画データは電子メールの添付ファイルとして送受信される。

【 0 0 3 8 】

ファクシミリサーバ 1 は、アナログの公衆電話回線網（PSTN）3 にも接続されており、LAN 5 により接続されたコンピュータネットワークにおけるクライアントコンピュータ 4 のサーバコンピュータとして機能する。具体的にはファクシミリサーバ 1 は、クライアントコンピュータ 4 からの電子メールによる要求に応じてファクシミリメッセージ（画データ）を PSTN 3 へ送信する機能、及び PSTN 3 から受信したファクシミリメッセージを電子メールによりクライアントコンピュータ 4 へ配信する機能等を少なくとも備えている。

ファクシミリサーバ 1 は、PSTN 3 においては、勧告 T. 3 0（一般交換電話網における文書ファクシミリ伝送のための手順）に従って作動する。

【 0 0 3 9 】

なお、本発明における電話回線網としては、一般の公衆電話回線網に限定するものではなく、例えば専用電話回線網であってもよい。

また、P S T N 3 にはそれぞれ電話番号が付与された多数のファクシミリ装置（図 6 では参照符号 2 にて一台のみ示されている）が接続されていることは言うまでもない。

なお、図 6 には 1 台のクライアントコンピュータ 4 が示されているが、最低限 1 台が L A N 5 に接続されていればよい。但し、実際にはより多数のクライアントコンピュータが L A N 5 に接続されている場合が多い。

本発明に係るファクシミリ装置であるファクシミリサーバ 1 の実施の形態 2 の構成は、上述した図 2 のブロック図と同様であるので、説明を省略する。

【 0 0 4 0 】

本発明に係るファクシミリ装置の実施の形態 2 としてのファクシミリサーバ 1 は、通常のファクシミリサーバとしての機能を有しているが、その他に親展受信したときに、例えば I D - N I K S による暗号化／復号によりクライアントコンピュータ 4 と通信する。I D - N I K S については、上述した（図 3）ので説明を省略する。

【 0 0 4 1 】

ファクシミリサーバ 1 及びクライアントコンピュータ 4 は、予め、センタにおいて、センタ公開情報 { P C _i }、センタ秘密情報 { S C _i } 及びそれぞれの L A N 5 におけるアドレスである I D 情報 h (I D _X) に基づいて、それぞれ秘密情報 S _{Xi} が計算され、秘密裏に配布され、記憶している。

ファクシミリサーバ 1 及びクライアントコンピュータ 4 は、L A N 5 における通信において、その通信相手との間で、暗号化、復号のための共通鍵 K _{XY} を、自身の秘密情報 { S _{Xi} }、センタ公開情報 { P C _i } 及び相手先の I D 情報 h (I D _Y) を用いて以下のように生成する。

$$K_{XY} = f (\{ S_{Xi} \} , \{ P C_i \} , h (I D_Y))$$

【 0 0 4 2 】

以下に、このような構成のファクシミリサーバ 1 の動作を、それを示すフロー

チャートを参照しながら説明する。

図7は、ファクシミリサーバ1が親展受信したときの動作を示すフローチャートであり、図8は、そのときのクライアントコンピュータ4の動作を示すフローチャートである。

ファクシミリサーバ1は、ファクシミリ装置2からPSTN経由で親展受信すると(図7S40)、自身の秘密情報、センタ公開情報、及びその親展受信の宛先であるクライアントコンピュータ4のLAN5におけるアドレスを用いて、暗号化、復号のための共通鍵を作成する(S42)。

【0043】

次に、ファクシミリサーバ1は、クライアントコンピュータ4へ親展受信したことを通知する為の通知文を、作成した共通鍵(S42)により暗号化し(S44)、暗号化した通知文を電子メールとしてLAN5経由でクライアントコンピュータ4へ送信し(S45)リターンする。

送信された電子メール(S45)は、メールサーバ6内のクライアントコンピュータ4のメールボックスに一旦記憶される。

【0044】

クライアントコンピュータ4は、メールチェックの指示が入力されると(図8S60)、メールサーバ6のメールボックスにファクシミリサーバ1からの電子メールが記憶されていないかメールチェックを行い(S62)、ファクシミリサーバ1からの電子メールが記憶されていなければ(S64)リターンする。

【0045】

クライアントコンピュータ4は、メールチェックを行い(S62)、ファクシミリサーバ1からの電子メールが記憶されており配信されて来たときは(S64)、ファクシミリサーバ1のLAN5におけるアドレスを用いて、暗号化、復号のための共通鍵を作成する(S66)。

次に、クライアントコンピュータ4は、受信した電子メール(S64)を、作成した共通鍵(S66)により復号して表示する(S68)。

クライアントコンピュータ4は、復号して表示した電子メール(S68)が親展受信の通知でないときは(S70)リターンする。

【0046】

クライアントコンピュータ4は、受信した電子メール（S64）を復号して表示している（S68）状態で、ユーザによりその応答内容が入力されると（S72）、その応答内容を、作成した共通鍵（S66）により暗号化し（S74）、暗号化した応答内容を電子メールとしてLAN5経由でファクシミリサーバ1へ送信し（S76）リターンする。

送信された（S76）電子メールは、メールサーバ6内のファクシミリサーバ1のメールボックスに一旦記憶される。

クライアントコンピュータ4は、受信した電子メール（S64）を復号して表示している（S68）状態で、ユーザによりその応答内容が入力されないままに（S72）、所定時間が経過したときは（S84）リターンする。

【0047】

ファクシミリサーバ1は、周期的に実行するメールサーバ6へのメールチェックにより、4クライアントコンピュータ4から電子メールを受信すると（図7S46）、自身の秘密情報、センタ公開情報、及びその電子メールの送信元であるクライアントコンピュータ4のLAN5におけるアドレスを用いて、暗号化、復号のための共通鍵を作成する（S48）。

次に、ファクシミリサーバ1は、作成した共通鍵（S48）により、受信した電子メール（S46）を復号する（S50）。

【0048】

ファクシミリサーバ1は、復号した電子メールの応答内容（S50）が、親展受信した画データ（S40）の配信要求であれば（S52）、親展受信した画データ（S40）を、作成した共通鍵（S48）により暗号化し（S54）、電子メールの添付ファイルとしてクライアントコンピュータ4へ配信する（S56）。

配信された（S56）電子メールは、メールサーバ6内のクライアントコンピュータ4のメールボックスに一旦記憶される。

ファクシミリサーバ1は、復号した電子メールの応答内容（S50）が、親展受信した画データ（S40）の配信要求でなければ（S52）リターンする。

【0049】

クライアントコンピュータ4は、メールチェックの指示が入力されると（図8 S60）、メールサーバ6のメールボックスにファクシミリサーバ1からの電子メールが記憶されていないかメールチェックを行い（S62）、ファクシミリサーバ1からの電子メールが記憶されていなければ（S64）リターンする。

【0050】

クライアントコンピュータ4は、メールチェックを行い（S62）、ファクシミリサーバ1からの電子メールが記憶されており配信されて来たときは（S64）、ファクシミリサーバ1のLAN5におけるアドレスを用いて、暗号化、復号のための共通鍵を作成する（S66）。

次に、クライアントコンピュータ4は、受信した電子メール（S64）を、作成した共通鍵（S66）により復号して表示し（S68）、表示した内容が画データであれば（S70）リターンする。

尚、クライアントコンピュータ4から配信要求するときに、パスコードも入力して送信し、ファクシミリサーバ1側でそのパスコードの正誤を判定し、正しいと判定したときに、画データを送信するようにしても良い。

【0051】

また、上述した実施の形態2においては、ファクシミリサーバ1が親展受信し一旦記憶した情報の宛先である親展処理すべきコンピュータへ電子メールにより通知し、その電子メールを見たユーザがコンピュータから、自分のメールボックスへ送信させるように指示しているが、ファクシミリサーバ1は、親展受信し一旦記憶した情報を、自動的に電子メールで送信するように、親展受信がある都度送信するように、何通か溜まったときに送信するように、指定時刻になったときに送信するように、それぞれ設定しておくことが可能である。

【0052】

図9は、ファクシミリサーバ1が親展受信したときに、親展受信した情報を自動的に電子メールで送信する場合の動作を示すフローチャートであり、図10は、そのときのクライアントコンピュータ4の動作を示すフローチャートである。

ファクシミリサーバ1は、ファクシミリ装置2からPSTN経由で親展受信す

ると（図 9 S 9 0）、自身の秘密情報、センタ公開情報、及びその親展受信の宛先であるクライアントコンピュータ 4 の LAN 5 におけるアドレスを用いて、暗号化、復号のための共通鍵を作成する（S 9 2）。

【 0 0 5 3 】

次に、ファクシミリサーバ 1 は、親展受信した情報（画データ）（S 9 0）を、作成した共通鍵（S 9 2）により暗号化し（S 9 4）、暗号化した画データを電子メールの添付ファイルとして LAN 5 経由でクライアントコンピュータ 4 へ配信し（S 9 6）リターンする。

配信された電子メール（S 9 6）は、メールサーバ 6 内のクライアントコンピュータ 4 のメールボックスに一旦記憶される。

【 0 0 5 4 】

クライアントコンピュータ 4 は、メールチェックの指示が入力されると（図 1 0 S 1 0 0）、メールサーバ 6 のメールボックスにファクシミリサーバ 1 からの電子メールが記憶されていないかメールチェックを行い（S 1 0 2）、ファクシミリサーバ 1 からの電子メールが記憶されていなければ（S 1 0 4）リターンする。

【 0 0 5 5 】

クライアントコンピュータ 4 は、メールチェックを行い（S 1 0 2）、ファクシミリサーバ 1 からの電子メールが記憶されており配信されて来たときは（S 1 0 4）、ファクシミリサーバ 1 の LAN 5 におけるアドレスを用いて、暗号化、復号のための共通鍵を作成する（S 1 0 6）。

次に、クライアントコンピュータ 4 は、受信した電子メール（S 1 0 4）を、作成した共通鍵（S 1 0 6）により復号して表示し（S 1 0 8）リターンする。

【 0 0 5 6 】

【発明の効果】

以上に詳述した如く第 1， 2 発明に係るファクシミリ装置によれば、ファクシミリ通信により親展受信した情報をその宛先である親展処理すべきコンピュータへ送信する際に、秘密を維持することが出来るファクシミリ通信を実現することが出来る。特に、暗号通信する際の予備的な相互通信が不要であり、手間を省く

ことが出来る。

【 0 0 5 7 】

第 3 発明に係るファクシミリ装置によれば、コンピュータネットワークの秘密保証の程度及び親展受信するであろう情報の内容に応じて、秘密保持の程度を定めておくことが出来る。

【図面の簡単な説明】

【図 1】

本発明に係るファクシミリ装置のコンピュータネットワークへの接続形態を示す模式図である。

【図 2】

本発明に係るファクシミリ装置としてのファクシミリサーバの構成を示すブロック図である。

【図 3】

I D - N I K S のシステムの原理を説明する為の説明図である。

【図 4】

本発明に係るファクシミリ装置の動作を示すフローチャートである。

【図 5】

クライアントコンピュータの動作を示すフローチャートである。

【図 6】

本発明に係るファクシミリ装置のコンピュータネットワークへの接続形態を示す模式図である。

【図 7】

本発明に係るファクシミリ装置の動作を示すフローチャートである。

【図 8】

クライアントコンピュータの動作を示すフローチャートである。

【図 9】

本発明に係るファクシミリ装置の動作を示すフローチャートである。

【図 1 0】

クライアントコンピュータの動作を示すフローチャートである。

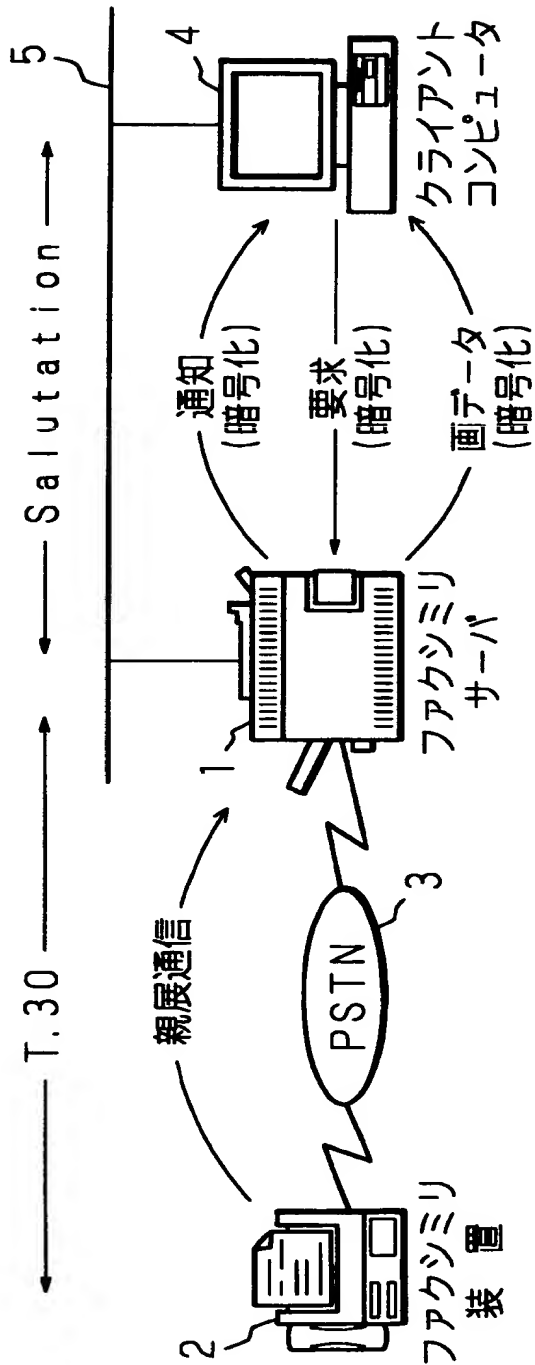
【符号の説明】

- 1 ファクシミリサーバ（ファクシミリ装置）
- 2 ファクシミリ装置
- 3 公衆電話回線網（P S T N）
- 4 クライアントコンピュータ（コンピュータ）
- 5 L A N
- 6 メールサーバ
- 1 0 C P U
- 1 1 P R O M
- 1 2 R A M
- 1 8 L A N I / F

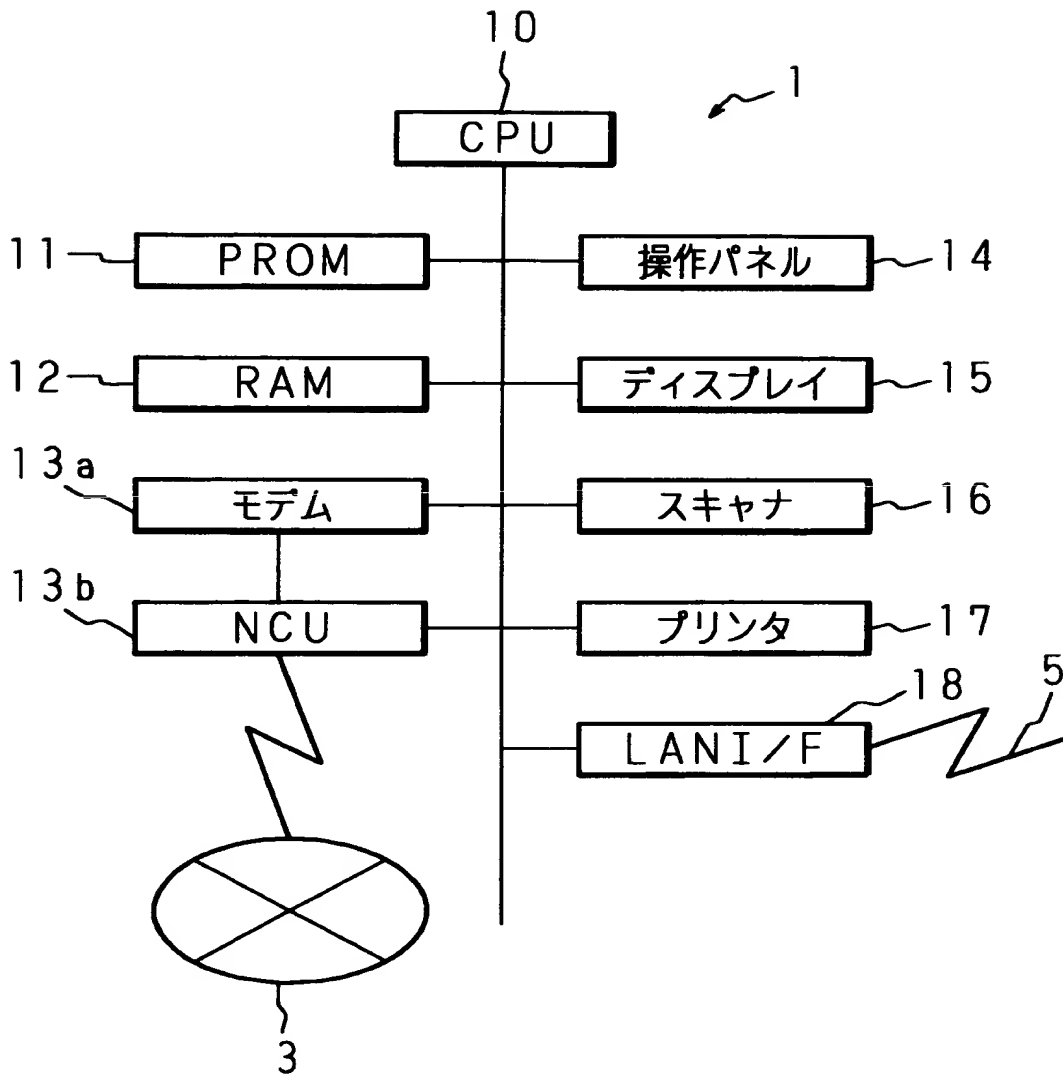
【書類名】

図面

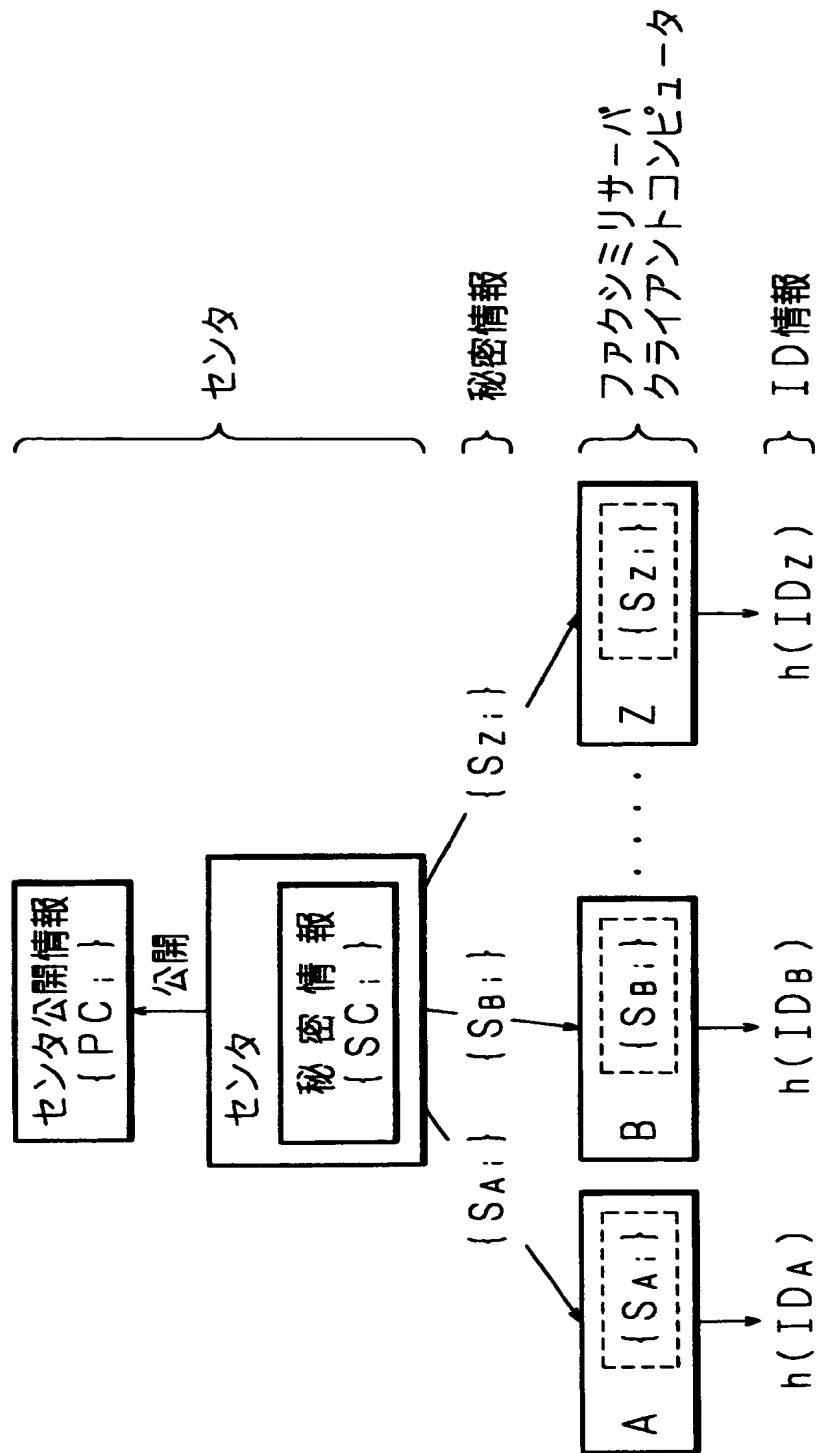
【図 1】



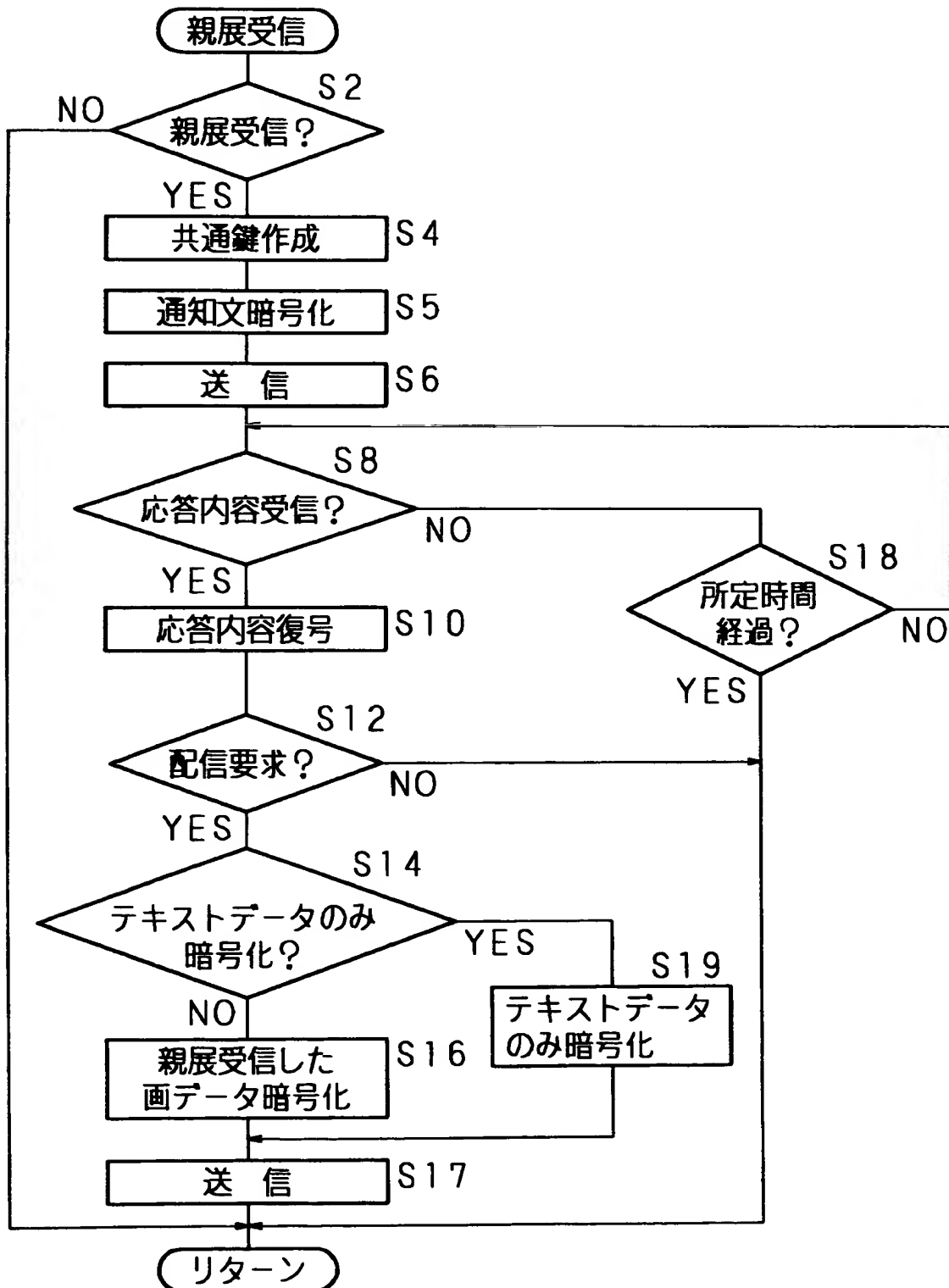
【図2】



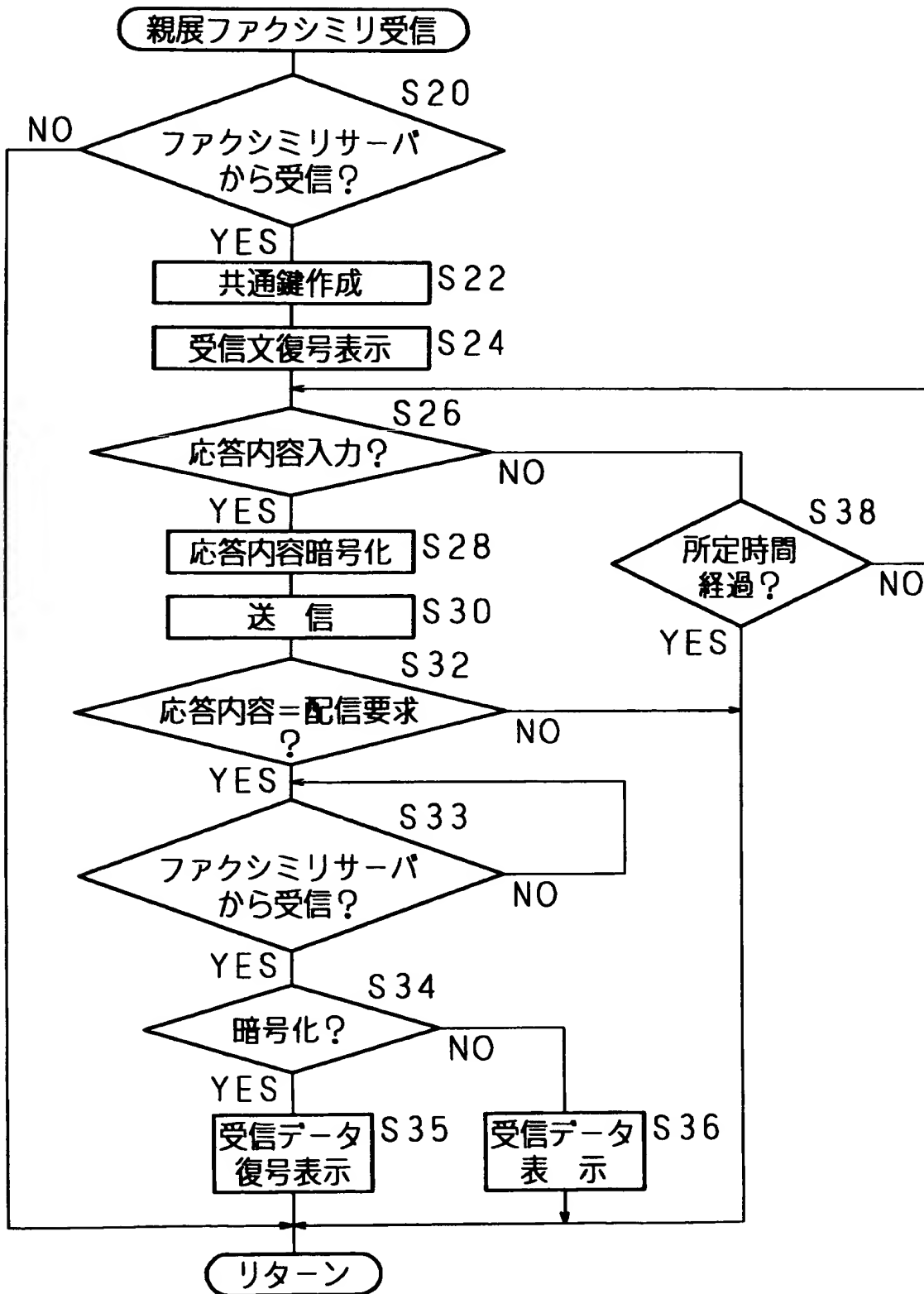
【図3】



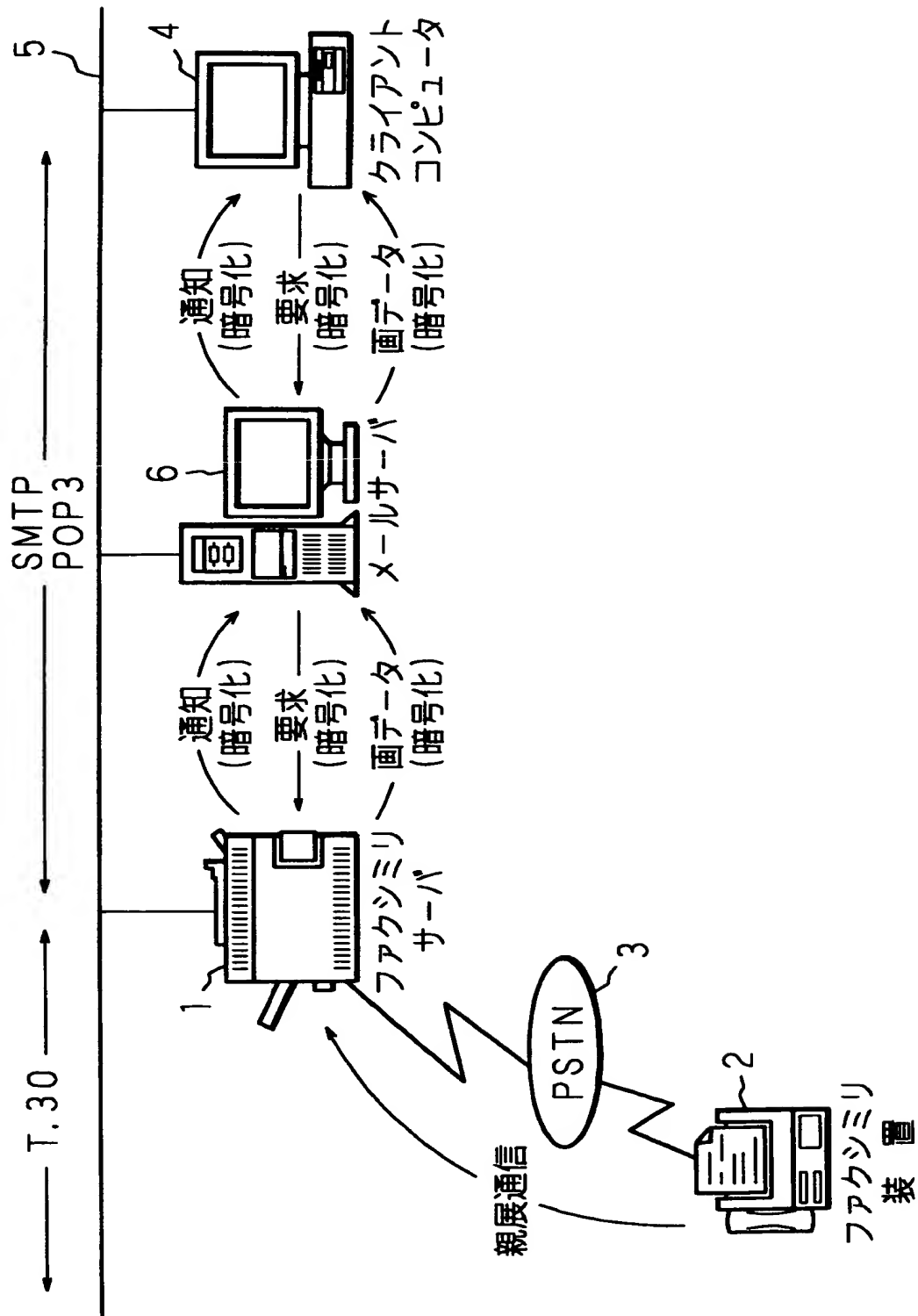
【図 4】



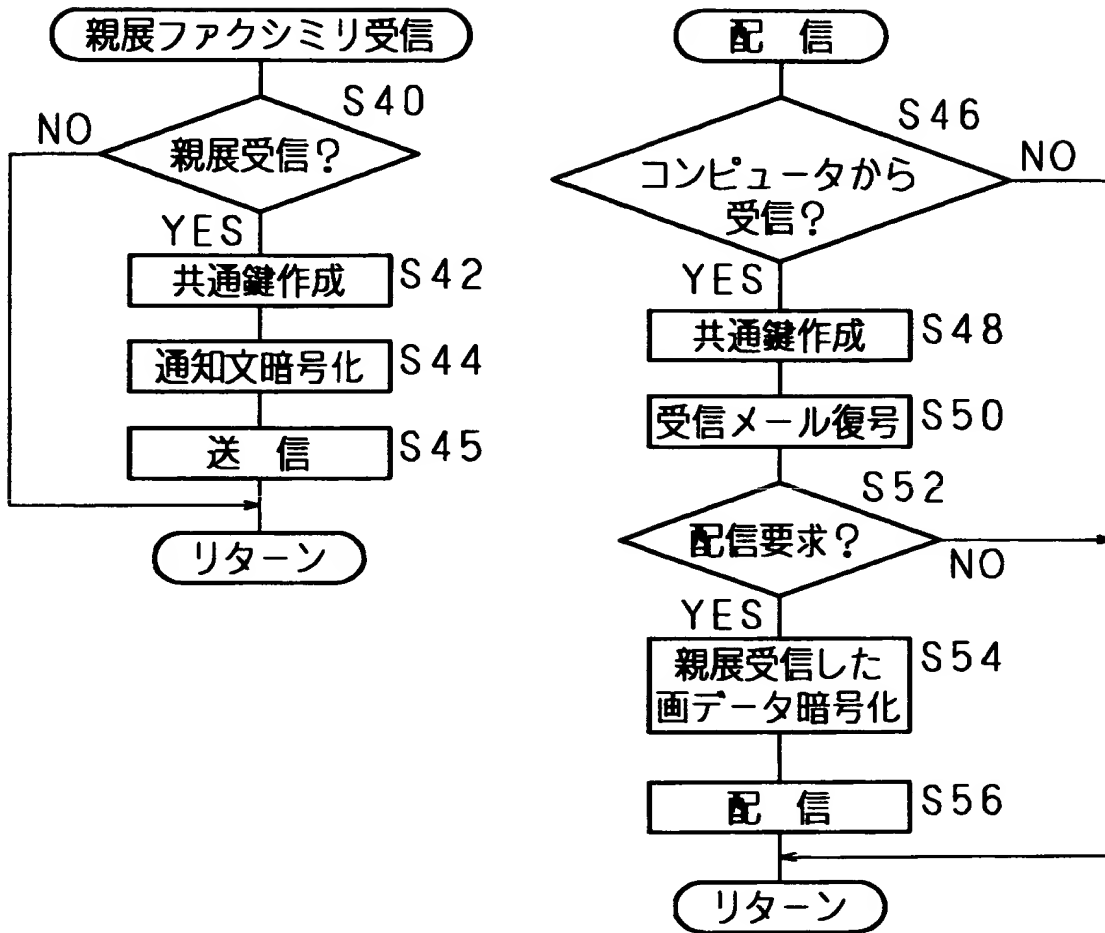
【図 5】



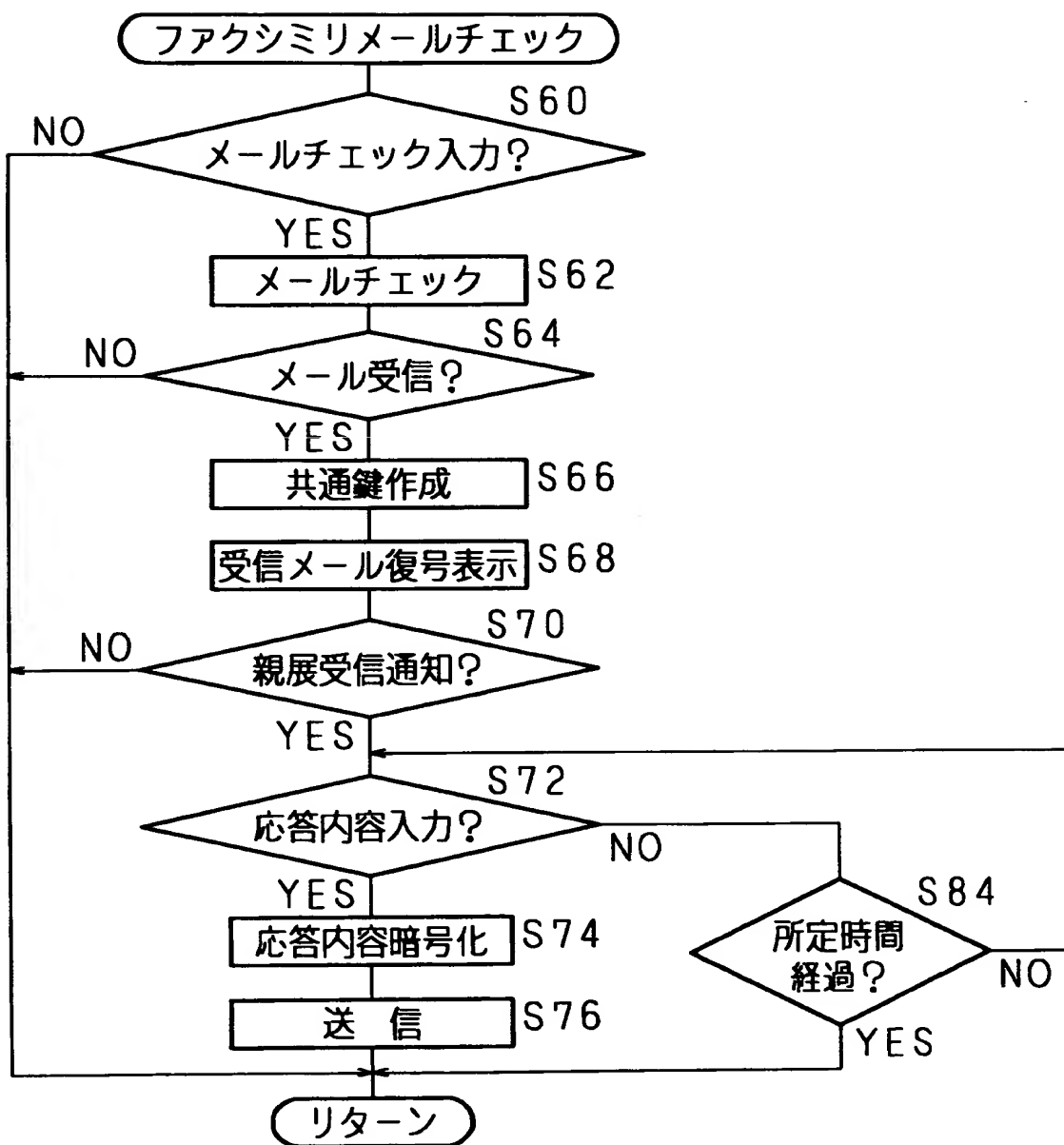
【図 6】



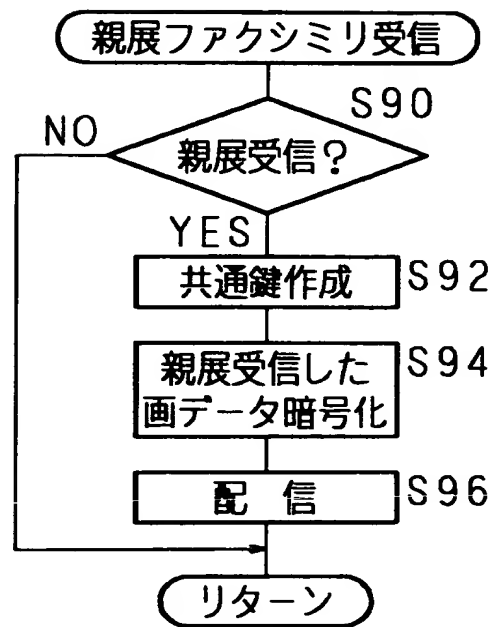
【図 7】



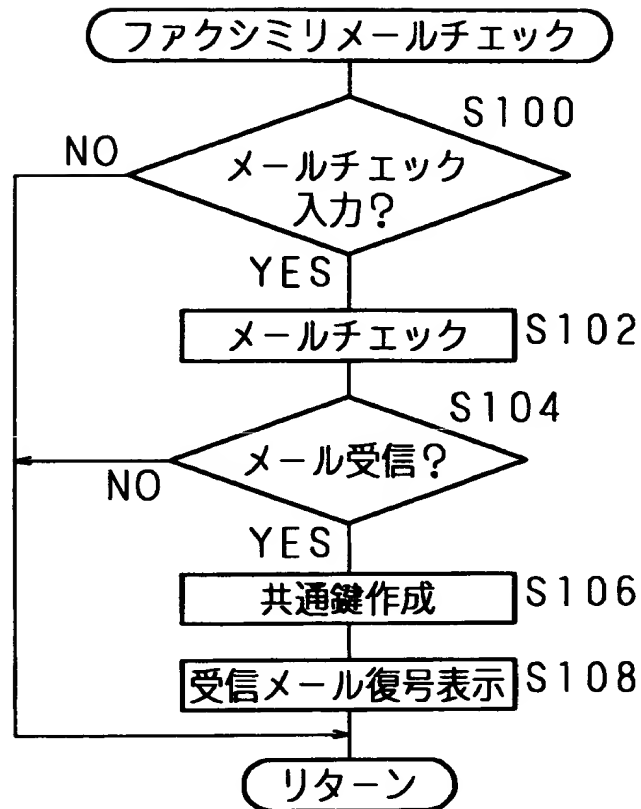
【図 8】



【図 9】



【図 10】



【書類名】 要約書

【要約】

【課題】 ファクシミリ通信により親展受信した情報をその宛先コンピュータへ送信する際に、秘密を維持することが出来るファクシミリ装置の提供。

【解決手段】 自身及び通信相手の各固有情報に基づく暗号鍵（S 4）により暗号化／復号し（S 5， 1 0， 1 6）ネットワークを介してコンピュータと通信し（S 6， 8， 1 7）、コンピュータの指示でファクシミリ通信を行なうファクシミリ装置。親展受信したときに（S 2）親展処理すべきコンピュータへ通知する手段（S 5， 6）と、そのコンピュータからの要求に応じて（S 8， 1 0， 1 2）親展受信（S 2）の内容を送信する手段（S 1 6， 1 7）とを備えている。

【選択図】 図 4

出 願 人 履 歴 情 報

識別番号 [000006297]

1. 変更年月日 1990年 8月 7日

[変更理由] 新規登録

住 所 京都府京都市南区吉祥院南落合町3番地
氏 名 村田機械株式会社